REMARKS

Claims 1 – 11 are pending in this application.

In an Office Action mailed 25 January 2007, the Examiner rejected claims 1 – 11 under 35 USC 102(e) as being anticipated by Asano et al. (US Patent Application Publication No. 2003/0095664, hereinafter "Asano"), noting with respect thereto:

As per claims 1, 5, 8 and 10:

Asano discloses a method for generating an encryption key comprising:

retrieving the host identification from the host device for use as a private portion of an encryption key (paragraphs 0213 -0218);
generating at least one content variable that uniquely identifies a corresponding block of said file as a public portion of said encryption key (paragraph 0220, where the block seed is the content variable);
combining the host identification and the at least one content variable to produce the encryption key that was used to encrypt the file (paragraph 0220);
encrypting a block of plaintext data using the encryption key to produce a block of ciphertext (paragraphs 0245-0275);
appending only the at least one content variable to the block of ciphertext (0245-0275);
transmitting the block of ciphertext and the appended at least one content variable over the unsecured interface to the storage device (paragraphs 0245-0276);
storing the block of ciphertext and the appended one or more content variables within a storage device (paragraphs 0245-0276); and
decrypting the block of ciphertext with the encryption key to produce the block of plaintext (paragraphs 0276-0298).

The present method for encryption key generation provides a method of combining the speed of conventional encryption with the security of public key encryption. The host device encrypting the plaintext to be transmitted over the unsecured interface is assigned a host identification. The host identification is stored in a secure location within the host device. The host identification is analogous to the private key. Only the host device can generate the encryption key used to later decrypt the ciphertext. A second variable, a content identification, is generated by the host device. Each successive block of plaintext to be encrypted uses a different content identification. The host identification along with the content identification is used for generating an encryption key to encrypt a block of plaintext. This second variable, the content identification, is analogous to the public key. The content identification is transmitted with the resulting ciphertext and together the ciphertext and content identification are stored for retrieval at a later time. The

encryption key is never transmitted with the file and is only stored in the host device to ensure that only the host device can decrypt the encrypted file. The encryption key is generated following a method that can be repeated later using the same host identification and content identification to generate the same encryption key. In other words, the formula used to generate the encryption key is deterministic.

The cited reference US Patent Application Publication No. 2003/0095664 contains Figures 1-6, yet the sections [245-276] cited by the Examiner refer to non-existent Figures 23-28. Due to the lack of these figures, Applicant is unable to provide a proper response to the Office Action and hereby requests that the Examiner address the issue of the cited reference being incomplete.

In view of the above amendments and remarks, Applicant believes the pending application is in condition for allowance. Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-1848, under Order No. 013208.0121PTUS from which the undersigned is authorized to draw.

Respectfully submitted,
PATTON BOGGS LLP

Dated: 9 APRIL 2007

By: _____
James M. Graziano
Registration No.: 28,300
(303) 830-1776

(303) 894-9239 (Fax)
Attorney for Applicant

Customer No. 24283